



KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.



Privacy and Security

July 2017



Privacy and Security

This presentation will review Privacy and Security policies and best practices when working with applicants for Medicaid and Qualified Health Plans.

Introduction

It is of the utmost importance and a legal requirement to always be aware of the privacy and security of handling individuals' personal information.

While performing Agent and Assister duties, you will be exposed to sensitive client information, or Personally Identifiable Information (PII).

Agent and Assistors must handle PII carefully and should not leave it in public places or areas where others may be able to access it. When discarding PII, Agents and Assistors should use a shredder, not a trash can or recycling bin.

- There are serious legal and personal consequences to breaching privacy and security laws.
- It is important that you understand the overarching Federal guidelines in addition to internal office policies of the Kentucky Health Benefit Exchange.

HIPAA

Established in 1996, the Health Insurance Portability and Accountability Act (HIPAA) is a federal law that primarily aims to:

1. Make it easier for people to keep health insurance
2. **Protect the confidentiality and security of healthcare information**
3. Help the healthcare industry control administrative costs

HIPAA is comprised of various rules and regulations, which apply to covered entities and their business associates. Individuals, organizations, and agencies that meet the definition of a covered entity must comply with HIPAA's requirements to protect individually identifiable health information and provide patients with certain rights pertaining to that information. If a covered entity works with a business associate, the entity must have a contract or other arrangement with the business associate that establishes specifically what the business associate will do and requires the business associate to comply with the rules' requirements to protect the privacy and security of protected health information.

If covered entities and their business associates do not follow the HIPAA rules and regulations, they are directly liable and face severe penalties for the release of that information.

Covered Entity

Healthcare Provider

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

Please note that healthcare providers must transmit information in an electronic form in connection with a transaction that falls under the HIPAA standards. Also, government programs that pay for healthcare include Medicare, Medicaid, and the military and veterans' healthcare programs.

Health Plan

- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for healthcare

Healthcare Clearinghouse Business Associates

This includes entities that process nonstandard health information that they receive from another entity into a standard electronic format or data content, or vice versa.

HIPAA Rules and Regulations

Privacy Rule	<ul style="list-style-type: none">• Establishes national standards to protect individuals' medical records and other personal health information
Security Rule	<ul style="list-style-type: none">• Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity• Requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information
Enforcement Rule	<ul style="list-style-type: none">• Contains provisions relating to compliance and investigations, the imposition of civil money penalties for violation of the HIPAA Administrative Simplification Rules, and procedures for hearings

HIPAA Rules and Regulations

Breach Notification Rule	<p>Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information</p> <p>Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers.</p>
Transactions and Code Sets Standards	<p>Creates a uniform way to perform electronic data interchange (EDI) transactions for submitting, processing, and paying claims.</p>
Employer Identifier Standard	<p>Requires employers have standard national numbers that identify them on standard transactions. The Employer Identification Number (EIN) is the identifier for employers and is issued by the Internal Revenue Service (IRS).</p>
National Provider Identifier (NPI) Standard	<p>The NPI is a unique identification, 10-digit number for covered healthcare providers. Covered healthcare providers and all health plans and healthcare clearinghouses must use NPIs in the administrative and financial transactions adopted under HIPAA.</p>

Protected Health Information (PHI) and Personally Identifiable Information (PII)

The HIPAA Privacy Rule purpose is to protect Individually Identifiable Health Information (IIHI). This information is also known as Protected Health Information or (PHI) and is a subset of Personally Identifiable Information (PII) which is discussed below.

For information to be considered PHI, it must meet all of the following conditions:

1. The information is created, received, or maintained by a health provider or health plan.
2. The information is related to past, present or future healthcare or payment for that healthcare.
3. The information identifies a member or patient, or there is enough information to be able to identify the individual.

Protected Health Information (PHI) and Personally Identifiable Information (PII)

Individually Identifiable Health Information includes many common identifiers, such as name, address, birth date, and Social Security Number.

HIPAA regulations do not provide a list of information that is defined as IIHI.

Below are direct identifiers of a limited data set. These identifiers are accepted in the healthcare field as being protected health information. This includes:

- (i) Names;
- (ii) Postal address information, other than town or city, state, and zip code;
- (iii) Telephone numbers;
- (iv) Fax numbers;
- (v) Electronic mail addresses;
- (vi) Social security numbers;
- (vii) Medical record numbers;
- (viii) Health plan beneficiary numbers;
- (ix) Account numbers;
- (x) Certificate/license numbers;
- (xi) Vehicle identifiers and serial numbers, including license plate numbers;
- (xii) Device identifiers and serial numbers;
- (xiii) Web Universal Resource Locators (URLs);
- (xiv) Internet Protocol (IP) address numbers;
- (xv) Biometric identifiers, including finger and voice prints;
- (xvi) Full face photographic images and any comparable images

Protected Health Information (PHI) and Personally Identifiable Information (PII)

Personally Identifiable Information (PII)

As previously mentioned, PHI is a subset of Personally Identifiable Information (PII). PII is defined as information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

The generally accepted set of individually unique data elements in PII include the following list:

Data Element	Description
Name	First name, last name, maiden name combinations. It could be possible to identify an individual using a combination of data e.g. first name, zip code, street address etc.
Geographic locators	Street address, city, precinct, zip code, latitude and longitude coordinates, etc.)
Dates	Significant events in an individual's life - birth, death, marriage, admission, discharge, etc. The year is generally considered fine for use except in the case of the very elderly (>89 years of age; in which case they would be represented by an aggregate category e.g. =>90)
Phone numbers	Personal, work, other mobile or land line numbers linked to an individual

Protected Health Information (PHI) and Personally Identifiable Information (PII)

Personally Identifiable Information (PII) continued:

Data Element	Description
Fax numbers	Same as above
Electronic mail addresses (email)	Same as above
Social Security Number	9-digit number that continuously links an individual to his/her Social Security
Medical record numbers	Medical record numbers can be used to identify individuals if one also knew the institution that assigned it
Health plan beneficiary numbers	Insurance card/member ID
Account numbers	Bank numbers, etc
Certificate/license numbers	Driver's license, birth certificate, etc

Protected Health Information (PHI) and Personally Identifiable Information (PII)

Personally Identifiable Information (PII) continued:

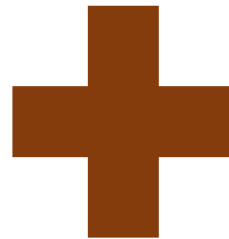
Data Element	Description
Vehicle identifiers and serial numbers, including license plate	Any vehicle characteristic that can help track down an individual
Device identifiers and serial numbers	Medical devices with unique serial numbers, personal electronics, etc
Web Universal Resource Locators (URLs)	Technology can now track individuals' locations and identities based on browser history and web site visits
Internet Protocol (IP) address numbers	Similar to above
Biometric identifiers, including finger and voice prints	Retinal images also fall into this category
Full face photographic images and any comparable images	Visual aids that identify who you are

Protected Health Information (PHI) and Personally Identifiable Information (PII)

The Kentucky Revised Statutes of the Kentucky Legislature, 61.931, further clarifies Personal Information to be:

One of the following:

- **First name and last name**
- **First initial and last name**
- **Personal mark**
- **Unique biometric**
- **Genetic print or image**



In combination with one or more of the following data elements:

- An account number
- Credit card number or debit card number with required security or access code or password, that grants access to the account
- Social Security number
- Taxpayer identification number
- Social Security number
- Driver's license number
- State identification card or other individual identification number issued by any agency
- Passport number
- Other identification number issued by the US government
- Individually identifiable health information as defined in 45 CFR 160.103 except for education records covered by the Family Educational Rights and Privacy Act.

Protected Health Information (PHI) and Personally Identifiable Information (PII)

As you can see, the internal office policies and procedures of Kentucky are based on the overarching guidelines set forth by the Federal government.

As Agents and Assisters, you will have access to this type of information when helping individuals and businesses apply for health coverage.

It is critical for you to know that personal information must be safeguarded

Best Practices:

- **Papers or copies containing PII should never be left unsecure.**
- **Shred documents once you have completed work with them.**
- **Password protected computer.**
- **Locking your computer when away from the screen.**
- **Do not repeat PII aloud during an interview if others are nearby or could hear you over a phone call.**
- **Do not share PII unless there is a business need.**

Security Breaches

Defining a security breach

A security breach is the unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that has resulted in or is likely to result in the misuse of personal information.

If the agency has reason to believe that the records or data subject to the unauthorized access may compromise the security, confidentiality, or integrity of the personal information and has resulted in or is likely to result in the misuse of the personal information or likelihood of harm to one or more individuals, then the occurrence will be considered a security breach.

Security Breaches

Third party business partners of the Kentucky Office of the Health Benefit Exchange (KOHBE) are responsible for ensuring the security of emails sent to KOHBE if the email contains confidential or personal information.

KOHBE business partners must use secure email if sending confidential information to KOHBE staff.

Sending both a case number and name via email is a violation of PII.

Please note the importance of clearing your desk of confidential data files and papers at the end of the day.



ID Proofing

This section will review the purpose of ID Proofing and the process for successfully completing this important step with applicants.

Identity Proofing

Identity Proofing (ID Proofing): Verifying individual information

Because IHI and PII are extremely sensitive and important, it is critical for you as Agents and Assisters to verify the identity of who you are assisting.

Identity proofing is a federal requirement and a necessary step in facilitating enrollment. The information provided to benefit is sensitive Personally Identifiable Information, requiring a rigorous online verification process. Determining eligibility involves sensitive federal and state data, and benefit must verify individuals' identities before granting them full access to the system.

ID Proofing

There are three methods of verifying an individual's identity:

1. Provide the correct answers to a series of personal questions

It is important to note that Agent or Assistants will only have one attempt to correctly enter the individuals' answers to the Experian questions

2. Upload various forms of identification throughout the application process.

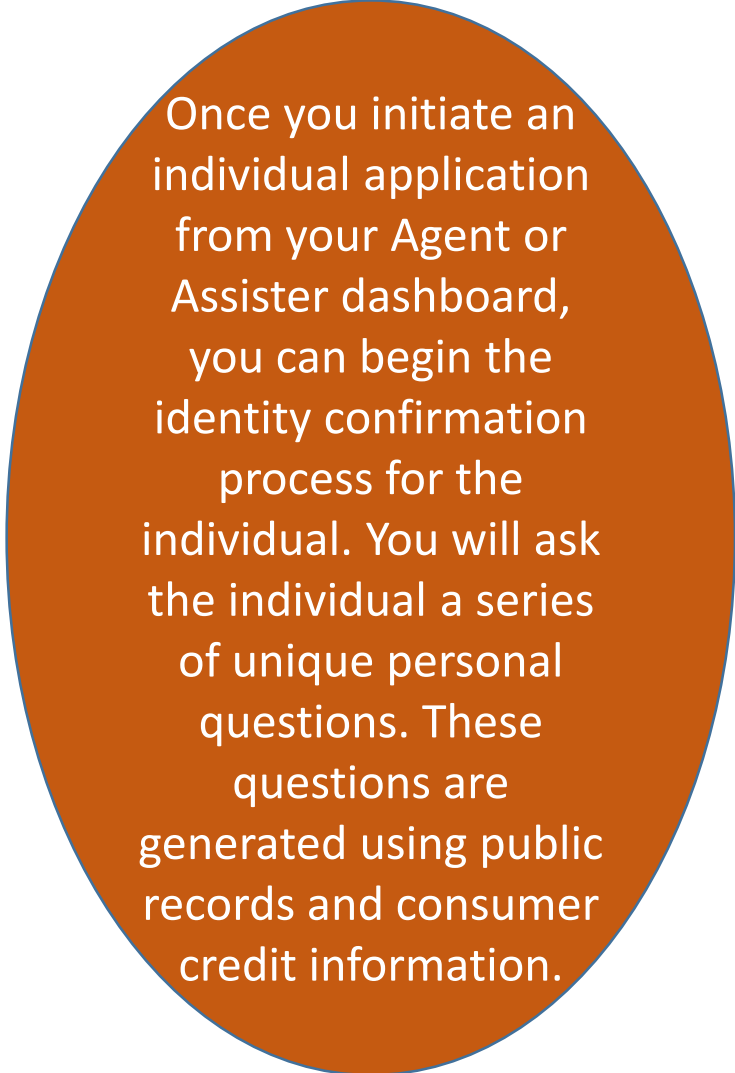
a) These forms of identification can include:

Adoption Record, Affidavit from non-US citizen, Affidavit from US citizen, Award Letter, Birth Record, Certificate of Tribal Affiliation, Certificate of US Citizenship (N- 560 or N-561), Incarceration Discharge Record, Divorce Decree, Driver's License, Employee ID, Federal Government issued ID, GED, Health Insurance Card, High School or College Diploma, Immigration Document (Government Issued), Income Tax Return, Law Enforcement Records, Local Government Issued ID, Marriage License, Military Dependent's ID, Naturalization Certificate, Passport, Personal Records Showing Deductions, Property Deed or Title, School Photo ID, School Record, State Government Issued ID, US Coast Guard Merchant Mariner card, US Military ID Card or Draft Record, and Wage Stubs

3. If the individual fails to correctly answer the Experian questions, they will be provided with a reference number and will need to call the Experian Help Desk at 1 (866) 578-5409. They will have to provide their last name, date of birth, and the reference number.

Using the KOG-Confirm Identity Tools Link

As an Agent or Assister assisting individuals with an application, it is a mandatory requirement to use the KOG-Confirm Identity Tools link to verify an individual's identity.

An orange oval graphic with a thin blue border, containing text about the identity confirmation process.

Once you initiate an individual application from your Agent or Assister dashboard, you can begin the identity confirmation process for the individual. You will ask the individual a series of unique personal questions. These questions are generated using public records and consumer credit information.

After you have begun an application, the Primary Applicant-Basic Information page displays.

- Enter the individual's first name, last name, date of birth, gender, and application channel.
- Click the KOG-Confirm Identity Tools link at the bottom of the page to verify the individual's identity.
- You can either confirm an individual's identity through this process or upload identification documents later.

ID Proofing

[Overview](#) [Messages](#) [Settings](#)

Primary Applicant - Basic Information

*=Required field

Below, please enter the personal information for the primary applicant of this application.

* First Name	M.I.	* Last Name	Suffix
<input type="text"/>	<input type="text"/>	<input type="text"/>	--Select-- <input type="button" value="v"/>
* Date of Birth (MM/DD/YYYY)	* Gender	* Channel	
<input type="text"/>	<input type="radio"/> Male <input type="radio"/> Female	--Select-- <input type="button" value="v"/>	

Providing a Social Security Number is not required at this point. However, if the primary applicant has a social security number and is applying for coverage, it will be required later on. Giving it now may reduce the number of steps you have to complete.

Email Address

Social Security Number(SSN)	Confirm Social Security Number (SSN)
<input type="text"/>	<input type="text"/>

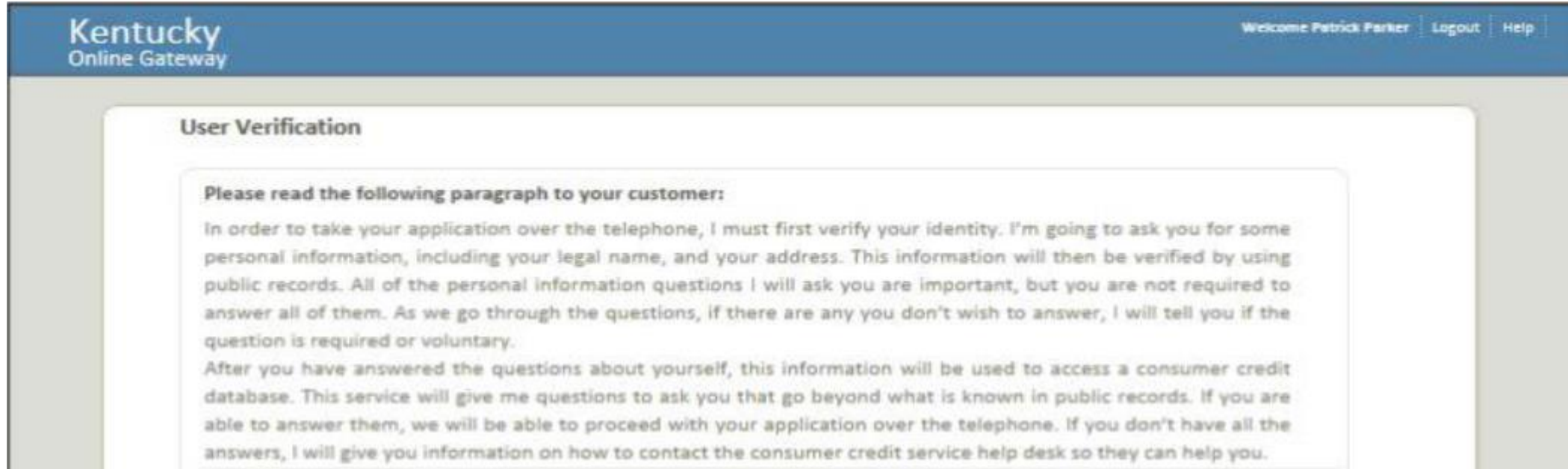
[KOG - Confirm Identity Tools](#)

Click **KOG-Confirm Identity Tools** to confirm Andrew's identity *before* clicking **Next** and beginning the application

Identifier Information

On the following screens, we will see the Kentucky Online Gateway (KOG) website displays. KOG uses public records and consumer credit information to verify an individual's identity before issuing health insurance.

Read the statement at the top of the page to the individual to inform them of this verification process. The individual must say yes before you can continue.



ID Proofing

Enter the individual's name, DOB, SSN, and home address.

* Legal First Name	John
Middle Name	Q
* Legal Last Name	Public
Name Suffix	<input type="text"/> ▼
* Birth Date	Jul ▼ 04 ▼ 1976 ▼
Social Security Number	●●●●●●●●
* Home Address	123 Main Street
* City	Capital City
* State	Kentucky ▼
* Postal Code	01234
Postal Extension Code	1234
Phone Number	8009762223

ID Proofing

Check the box to indicate that the individual agrees to the identity proofing terms and conditions and click **Next**.

The screenshot shows a web form for identity proofing. At the top, a line of text reads: "to the Customer: This request for identity proofing services is regulated by the Fair Credit Reporting Act. This service will be used solely to confirm your identity to avoid fraudulent transactions in your name." Below this, a question asks: "Do you understand and agree to this process?". A small, empty square checkbox is positioned directly under this question. A callout box with an orange border and a pointer to the checkbox contains the text "Check the box". Below the checkbox, a section titled "Do not read this to the customer: By checking this box, I certify that I:" is followed by a bulleted list of three items: "• understand this service is regulated by the Fair Credit Reporting Act;", "• am accessing this service on behalf of a customer who has requested my assistance for a valid purpose under my or my company's agreement with [redacted] and Family Services; and", and "• am requesting this service after [redacted] from the customer." A second callout box with an orange border and a pointer to the "Next" button at the bottom contains the text "Click Next". The "Next" button is a green rectangle with white text. To its left is a grey "Cancel" button with a left-pointing arrow. In the bottom right corner, the text "Identity proofing is enabled by" is followed by the Experian logo, which consists of a blue and red pixelated square icon and the word "Experian" in blue.

to the Customer: This request for identity proofing services is regulated by the Fair Credit Reporting Act. This service will be used solely to confirm your identity to avoid fraudulent transactions in your name.

Do you understand and agree to this process?

☐

Do not read this to the customer: By checking this box, I certify that I:

- understand this service is regulated by the Fair Credit Reporting Act;
- am accessing this service on behalf of a customer who has requested my assistance for a valid purpose under my or my company's agreement with [redacted] and Family Services; and
- am requesting this service after [redacted] from the customer.

Identity proofing is enabled by  Experian

[← Cancel](#) [Next](#)

ID Proofing

Examples of questions an individual might be asked are:

please select the county you have previously resided in, or which of the following represents the last four digits of your cellular phone number?

Note that these questions are unique to each individual based on public record or their credit history. If the individual does not have sufficient credit history, you may use the third manual ID proofing option mentioned earlier.

- Provide answers to each question.
- Click Next.

User Verification

* 1) You may have opened a mortgage loan in or around January 2013. Please select the lender to whom you currently make your mortgage payments. If you do not have a mortgage, select "NONE OF THE ABOVE/DOES NOT APPLY".

- ☐ PRUDENTIAL HOME MORTGAGE
- ☐ TD BANK
- ☐ COLONIAL SAVINGS & LOA
- ☐ FHLMC FREDDIE MAC
- ☐ NONE OF THE ABOVE/DOES NOT APPLY

* 2) Please select the city that you have previously resided in.

- ☐ LUVERNE
- ☐ HARVEST
- ☐ LEXINGTON
- ☐ LEEDS
- ☐ NONE OF THE ABOVE

* 3) You currently or previously resided on one of the following streets. Please select the street name from the following choices.

- ☐ KEYSTONE
- ☐ SMITHFIELD
- ☐ PRICE
- ☐ LIMESTONE
- ☐ NONE OF THE ABOVE

* 4) Which of the following represents the last four digits of your cellular phone number?

- ☐ 0752
- ☐ 7194
- ☐ 062
- ☐ 062
- ☐ NONE OF THE ABOVE

Click Next

Next

ID Proofing

If the individual provides the correct answers to all of his or her verification questions you can continue with his or her application on benefind.

Should the individual you are assisting fail the online ID proofing, he or she will receive a reference number.

Instruct him or her to call the Experian Helpdesk at 1 (866) 578-5409 for assistance and troubleshooting.

If the individual you are assisting answers the identity proofing questions incorrectly, you **will not be able to proceed with his or her application** until this issue is resolved.

ID Proofing

There is also a manual identification proofing option for those without credit history or those unable to pass the Experian identity proofing.

These individuals may be manually identity proofed by sending a copy of a photo ID, contact information, and a signed written statement by a supervisor to DMS.eligibility@ky.gov with “Request manual identity proofing” in the subject line.

You may also call 502-564-6890 and ask for RIPD assistance.

DMS office staff may contact the individual and or supervisor for additional information before approval. Please note that this process is available to Assisters only and that the information should be sent to contracted agencies only.



Penalties and Violations

In this section, we will review the consequences of violating privacy rules and procedures.

Penalties and Violations:

Civil Penalties	Criminal Penalties
Single violation of a provision, or multiple violations of different provisions could amount to a \$25,000 fine.	
Violations due to reasonable cause and not willful neglect of an identical requirement or prohibition during a calendar year, will provoke a \$1,000 fine for each violation, not exceeding \$100,000.	Wrongful disclosure of Individually Identifiable Health Information can incur a maximum fine of \$50,000 with up to 1 year of imprisonment.
Multiple violations due to willful neglect, not corrected, of an identical requirement or prohibition made during the same calendar year can lead up to a \$1.5 million fine.	Wrongful disclosure of Individually Identifiable Health Information committed under false pretenses could be up to a \$100,000 fine with up to 5 years of imprisonment.
Multiple violations due to willful neglect, not corrected, of an identical requirement or prohibition made during the same calendar year can lead up to a \$1.5 million fine.	Wrongful disclosure of Individually Identifiable Health Information (IIHI) committed under false pretenses with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm could be up to a \$250,000 fine with up to 10 years of imprisonment.

Additional Information and Resources

You may call Customer Service at 1 (855) 459-6328 for matters related to KHBE.

You can reach the Experian Helpdesk at 1 (866) 578-5409 for additional help and troubleshooting.

Specifically, if you'd like to submit a complaint, call 1 (887) 807-4027.

Office of Civil Rights (OCR)

The Office of Civil Rights (OCR) is a part of the U.S. Department of Health and Human Services (HHS). OCR enforces civil rights of healthcare providers receiving federal financial assistance from HHS. You can visit the OCR website at <https://www.hhs.gov/ocr/index.html>

U.S. Department of Health and Human Services (HHS)

The U.S. Department of HHS aims to improve the health, safety, and well-being of America. You can find more information on health information privacy at <https://www.hhs.gov/hipaa/index.html>



KENTUCKY HEALTH BENEFIT EXCHANGE
HEALTH INSURANCE
IS FOR EVERYONE. GET YOURS.



Thank you